BOIES SCHILLER FLEXNER

October 12, 2018

By ECF
Hon. Cathy Seibel, U.S.D.J.
United States Courthouse
300 Quarropas Street (Courtroom 621)
White Plains, NY 10601-4150

Re: *Broidy Capital Management LLC v. Benomar*, No. 18-CV-6615-CS
Third Party Subpoenas Seeking Perishable Evidence

Dear Judge Seibel:

Pursuant to the Court's order at the pre-motion conference of October 10, 2018, I write on behalf of Plaintiffs to request permission to serve ten third-party subpoenas that seek perishable evidence at risk of being lost before December 21, 2018. *See* October 10, 2018 Minute Entry; October 10, 2018 Conference Tr. at 47:9-16. The ten subpoenas Plaintiffs seek to serve are listed below:

1. 1&1 Mail and Media (provider of email accounts, including accounts using the mail.com domain, used in attack against Plaintiffs);
2. Cloudinary (provider of cloud image storage used in attack against Plaintiffs);
3. Google (provider of email accounts and services used in attack against Plaintiffs);
4. LinkedIn (provider of social media services associated with attack against Plaintiffs);
5. Microsoft (provider of email accounts associated with attack against Plaintiffs);
6. Oath Inc. (provider of email accounts associated with attack against Plaintiffs);
7. PDR Ltd. d/b/a PublicDomainRegistry.com (provider of services for domains associated with attack against Plaintiffs);
8. Quadranet (provider of internet service associated with attack against Plaintiffs);
9. TinyURL (provider of link shortening services used in attack against Plaintiffs); and
10. Twitter (provider of social media services associated with attack against Plaintiffs).

Each of these companies provided one or multiple services that was utilized, victimized, or otherwise associated with the attack against Plaintiffs. Each therefore may be in the possession of perishable, admissible evidence, including registration information and computer usage logs, which will allow Plaintiffs to prove attribution at trial.

There are several reasons to believe that service of these ten subpoenas now would prevent the loss of relevant, perishable evidence. *First*, with respect to relevance, Plaintiffs' subpoenas to date (including prior subpoenas to some of these same companies) resulted in the production of relevant information. To date, and largely as a result of a subpoena served on TinyURL, Plaintiffs have demonstrated that the attack against them is associated with a global hacking conspiracy that targeted more than 1,200 individuals,[1] and that that global hacking conspiracy continued to operate at least through the first six months of 2018. Indeed, Plaintiffs have evidence demonstrating that at least some of the accounts involved in the attack remain active,

[1] *See* Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," *Bloomberg*, September 18, 2018, https://www.bloomberg.com/view/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about.

accounts that Plaintiffs have only recently learned they must subpoena. The recent hacking activities, and their broad international scope, make it difficult for the hackers to completely cover their forensic tracks. Uncovering those tracks, however, requires multiple and iterative subpoenas, often to the same company, each of which builds upon the information learned from ongoing discovery. This process is ongoing but not yet complete.

Second, Plaintiffs have already observed the attackers changing tactics and seeking to better obfuscate their identity as a result of Plaintiffs' investigation. As a result of media coverage and public filings in this and the California action, the scope of Plaintiffs' investigation is being demonstrated to the attackers. Information already received as part of the investigation shows the attackers taking steps to cover their tracks, creating a race between Plaintiffs gathering the information through legal channels, and the hackers attempting to hide or delete material data. For example, the hackers changed their methods of disseminating stolen material in response to Plaintiffs' ability to analyze those documents. Similarly, email accounts and domains used to perpetuate the attack, some of which have now been publicly disclosed, have been closed.

Third, preservation letters will be insufficient for three separate reasons: (i) hold letters do not prevent hackers from seeking to destroy illegally electronic evidence in a third-party's possession; (ii) in some cases, the purpose of the proposed subpoenas is to identify other electronic service providers or individuals whose identity is currently unknown to Plaintiffs and who may unknowingly possess relevant information ; and (iii) the subpoena targets allow users themselves to delete data (which then may or may not be available in back-ups depending upon the timing of when the information was deleted and when the back-up was run).

Two examples serve to illustrate the inadequacy of hold letters. Through discovery in the California action, Plaintiffs were able to identify an Internet Service Provider ("ISP") that provided internet services used to access Plaintiffs' computers without authorization. Plaintiffs subpoenaed that ISP and the documents produced in response identified two small businesses that had supplied internet services to the attackers. A hold letter to the ISP would not have served to preserve evidence at the two businesses that provided services to the attackers.

Similarly, as a result of piecing together evidence from multiple subpoenas—including a subpoena to Google that led to a subpoena to Verizon—Plaintiffs learned that the hackers had utilized the wireless networks of a small, independently owned restaurant in Harlem. To gain the relevant information from the Harlem restaurant, Plaintiffs visited it, received physical access to the router, and copied or examined files that the restaurant owners had no reason to know even existed. By doing so, Plaintiffs were able to connect that router directly with an illegal intrusion into a specific email account. There is no possibility that a hold letter could have preserved that information because without the multiple identifying subpoenas Plaintiffs would never have thought the attackers had used the wireless network of restaurants in Harlem, and also because the restaurant owners themselves would not have been able to identify or preserve the information on their own. Notably, the router in Harlem had once possessed additional relevant information that it had automatically deleted before Plaintiffs located it.

Fourth, the kind of electronic data sought by Plaintiffs is routinely overwritten or destroyed as part of normal business operations. Indeed, as the Harlem example shows, this has already

BSF

occurred. As an initial matter, the routine deletion of data is of concern as to companies possessing relevant information that Plaintiffs have not yet identified but hope to through these subpoenas. Moreover, the subpoena targets themselves also delete data as a matter of course. Seven of the identified companies specify periods in which they will delete data, including upon request of a user.[2] These policies have already prejudiced Plaintiffs. For example, Microsoft informed Plaintiffs that it permanently deletes email content and Internet Protocol Logs data associated with accounts that are closed or left inactive for approximately 270 days. Microsoft further deletes registration data after an additional 95 days. Similarly, LinkedIn informed Plaintiffs that it deletes information after six months. Plaintiffs were also unable to obtain requested information from Google because the accounts subpoenaed had been deleted and the relevant records purged. And these are just some examples of the ways in which routine data deletion has frustrated Plaintiffs' discovery efforts. Plaintiffs' fear of inadvertent data loss is thus supported both with respect to the subpoena targets themselves and also with respect to as-yet unknown parties that the subpoenas will identify.

Fifth, a delay until December actually pushes back Plaintiffs' data discovery (and the risk of data loss) much further. Plaintiffs' experience is that subpoenaed companies sometimes required months to respond to the subpoena, due to both corporate bureaucracy and the technical nature of the data sought by Plaintiffs. Re-starting discovery in December, therefore, would actually push the collection of responsive information well into 2019.

Given the issues outlined above, courts routinely allow early and expedited discovery against electronic service providers, even before resolving jurisdictional motions -- as was the case in the related California action. *E.g.*, *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 242 (S.D.N.Y. 2012) ("[E]xpedited discovery is necessary to prevent the requested data from being lost forever as part of routine deletions by the ISPs."); *see also In re Various Strike 3 Holdings, LLC Copyright Infringement Cases*, No. 17-cv-6717 (WFK) (CLP), 2018 WL 3404142, at *3 (E.D.N.Y. Jul. 11, 2018) (citing *Digital Sin*, 279 F.R.D. at 242); *Arista Records LLC v. Does 1-43*, No. 07-cv-2357-LAB, 2007 WL 4538697, at *1 (S.D. Cal. Dec. 20, 2007).

For these reasons, Plaintiffs request permission to serve subpoenas against the ten companies identified above. Granting this request will safeguard against the irreparable harm that would follow the destruction of perishable admissible evidence, while imposing no appreciable burden on Defendant.

---

[2] *See*, "How Google Retains the Data We Collect", https://policies.google.com/technologies/retention?hl=en (Google users may delete data "whenever you like" and deletes other data within 9 months and 18 months); "Privacy Policy", https://www.linkedin.com/legal/privacy-policy (LinkedIn deletes account data within 30 days of closure). "Data protection with mail.com's Email," https://www.mail.com/company/data-collection/8537828-privacy-mailcom-mail.html#.8537822-stage-link1-1 (Mail.com deletes "[c]ontent and usage data after 180 days of inactivity."); "What happens to your data if you leave the service", https://www.microsoft.com/en-us/trustcenter/privacy/you-own-your-data (Microsoft deletes data 90 days after the termination or expiration of an account); "Data Storage and Anonymization", https://policies.oath.com/us/en/oath/privacy/topics/datastorage/index.html (Oath routinely deletes account one month after a request); "Privacy Policy", https://www.endurance.com/privacy/privacy (PDR Ltd. will retain some personal information up to seven years, but not addressing log data); "Privacy Policy", https://twitter.com/en/privacy (Twitter retains log data for up to 18 months). The remaining three companies do not state retention policies, but are believed to employ similar deletion protocols. *See generally* Agnieszka McPeak, "Disappearing Data," 2018 WIS. L. REV. 17, 21 (2018) ("Routine, good-faith deletion of ESI is a necessary business practice within companies.").

BSF

Respectfully submitted,

/s/Lee S. Wolosky

Lee S. Wolosky